



ELECTRONIC MESSAGING ASSOCIATION

February 5, 1997

Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
U.S. Department of Commerce
14th Street and Pennsylvania Ave., NW Rm. 2705
Washington, DC 20230

Dear Ms. Crowe:

The Electronic Messaging Association ("EMA") respectfully submits the attached comments on the interim regulation printed by the Commerce Department's Bureau of Export Administration ("BXA") in the Federal Register on December 30, 1996.

EMA consists of over 550 corporate and non-corporate members who are both users and providers of electronic messaging and electronic commerce products and services. Members include, Time Incorporated, Citicorp, Exxon, Lockheed, Ford, Hewlett-Packard, AT&T, Pfizer and many other organizations, large and small. User members reflect the proliferation of electronic messaging into virtually all areas of commerce. Provider members are involved in all phases of the technology, including software development, computer manufacturing, local and network messaging and global public and private network services. Both user members and provider members are keenly interested in encryption.

EMA believes U.S. businesses, particularly multinational corporations, need to be able to use and export robust encryption technology in order to retain their customers' confidence, compete in the global marketplace and continue their world leadership in technology development and use. Companies should be free to archive encryption keys and to use the most robust form of encryption necessary to protect customer assets and communications, including electronic financial transactions.

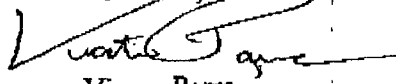
EMA is concerned that the interim rule of December 30 moves the Administration closer to third-party escrow as the only practical form of key recovery. EMA believes company employees must be eligible to act as key recovery agents and that BXA's regulations should expressly assure and protect that eligibility. Some companies may choose third-party recovery agents, but the regulations should not so clearly favor such an outcome.

#44
pg 189

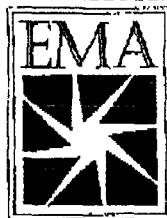
039

We look forward to hearing from you and the Administration and would be delighted to discuss this critical issue further.

Sincerely,

A handwritten signature in black ink, appearing to read "Victor Parra", written over a horizontal line.

Victor Parra
President and Chief Executive Officer.



ELECTRONIC MESSAGING ASSOCIATION

3 of 9

**COMMENTS OF THE ELECTRONIC MESSAGING ASSOCIATION
ON BXA'S DECEMBER 30, 1996
INTERIM RULE ON ENCRYPTION PRODUCTS**

The Electronic Messaging Association ("EMA") respectfully submits the following comments on the interim regulation printed by the Commerce Department's Bureau of Export Administration ("BXA") in the Federal Register on December 30, 1996.

EMA consists of over 550 corporate and non-corporate members who are both users and providers of electronic messaging and electronic commerce products and services. Members include, Time Incorporated, Citicorp, Exxon, Lockheed, Ford, Hewlett-Packard, AT&T, Pfizer and many other organizations, large and small. User members reflect the proliferation of electronic messaging into virtually all areas of commerce. Provider members are involved in all phases of the technology, including software development, computer manufacturing, local and network messaging and global public and private network services. Both user members and provider members are keenly interested in encryption.

EMA believes U.S. businesses, particularly multinational corporations, need to be able to use and export robust encryption technology in order to retain their customers' confidence, compete in the global marketplace and continue their world leadership in technology development and use. Companies should be free to archive encryption keys and to use the most robust form of encryption necessary to protect customer assets and communications, including electronic financial transactions.

EMA is concerned that the interim rule of December 30 moves the Administration closer to third-party escrow as the only practical form of key recovery. EMA believes company employees must be eligible to act as key recovery agents and that BXA's regulations should expressly assure

409

and protect that eligibility. Some companies may choose third-party recovery agents, but the regulations should not so clearly favor such an outcome.

Specific comments follow:

BXA's Summary

The introduction to the draft interim rule clearly discloses the Administration's intent to move toward a "worldwide key management infrastructure with the use of key recovery and key escrow encryption." Although the preamble introduces the draft interim rule as an implementation of the Vice President's October 1 speech, the draft interim rule actually goes substantially further towards making key escrow the backbone of the U.S. approach to the export of encryption-capable goods and systems.

By proposing that export licenses will be granted for periods of only six months, the draft interim regulation risks limiting the willingness of U.S. producers to bring products to market and U.S. multinationals to purchase and use such products. A six-month horizon is simply not enough. It would be preferable if, subject to revocation for cause, a BXA-reviewed product remained eligible for export for the entire proposed transition period, until January 1, 1999.

Moreover, not every potential exporter of encryption items will be in a position to make commitments to "build or market recoverable encryption items." U.S. companies with foreign subsidiaries and affiliates who are potential users of encryption items can only "build the supporting international infrastructure" by their international use of products conforming to the Administration's standards.

Supplementary Information: Background

Page 6: The inapplicability of the "publicly available" exception is handled in a confusing way. It is not at all clear why, simply because it appears in "software" form, object code that has been "published in a book or any other writing or media" should be excluded from the "publicly available" exception. It is of only minor comfort that the limitation applies only to encryption software controlled by the State Department prior to E.O. 13026. EMA prefers that the publicly

589

available exception apply. At a minimum, however, section 732.2 should be amended to remedy the confusion in the Supplementary Information. See also §§ 734.3(b)(2)(ii) and 734.7(b).

Page 6: The concept of "recovery encryption products" is absolutely central to the entire regulatory scheme, but the definition offered is inadequate. Among other things, the only "definition" is offered in the Supplementary Information section. Section 772 contains no definition of the concept. Elements of a possible definition appear in Supp. 4 to Part 742 under "Key Recovery Feature," but it is not apparent which of those elements would be essential to a definition.

Especially as the 1999 deadline approaches, users and potential customers will need to be able to assess independently which encryption products are "recoverable." It is our understanding that, for some industries and products, perhaps including certain integrated circuits and cellular telephone applications, full "recoverability" would not be necessary to the government's goals. Accordingly, a more precise definition of "recoverable" is essential to a workable set of regulations. At a minimum, the language in the Supplementary Information section should appear as a definition. Moreover, any definition of a key recovery product should remain neutral between recovery by employees or other agents of exporters and third-party recovery agents.

Proposed Regulations and Supplements

Part 734.2(b)(9)(i)(C): This clause requires anyone making encryption software available over electronic media, such as bulletin boards, to ensure that every party requesting or receiving a software transfer affirmatively acknowledge that the software is subject to export controls. Will BXA or other agencies investigating a transfer be content with a demonstration that a user's or transferor's system or facility does, in fact, require such affirmative acknowledgment, or does this provision contain, de facto, an additional recordkeeping requirement? It should not be the latter, but if BXA expects transferors to record and keep each acknowledgment, the regulations should be explicit on the point.

689

Section 740.8(d)(iv): It is difficult to understand exactly what EAR recordkeeping requirements would be applicable to key recovery agents. If key recovery agents are expected to maintain records beyond those mandated by Supp. 5 Part 742, "Key Recovery Procedures," item (2), such additional responsibilities should be spelled out. We are concerned, however, that maintaining, for up to five years, encyclopedic records of real-time communications-based exports could be unmanageable. Where appropriate, records of data generated by key recovery agents, especially when relating to information about third parties, should be expressly exempt from public disclosure.

Design, Implementation and Operational Assistance: Item (7) of this section prescribes that BXA-approvable encryption products "shall be resistant" to efforts to disable or circumvent stated key recovery and interoperability features. No manufacturer or user could guarantee such resistance. The ingenuity of computer and software engineers, including hackers, has been amply demonstrated. It would be preferable if the requirement were for key recovery products to "be designed to resist efforts to disable or circumvent ... "

Supp. 5 to Part 742: This supplement establishes the criteria for key recovery agents likely to be acceptable to BXA. BXA appears to expect that most key recovery agents will be third parties, persons or entities over whom users of encryption products will have no control. Such users can be subject to substantial business interruptions if the export licenses for the encryption productions on which the users depend are revoked because the government loses confidence in a key recovery agent. The regulations ought to go further to ensure that all reasonable steps will be taken to ensure that "decertification" of a key recovery agent does not penalize innocent users. The procedures in Supp. 5 to Part 742 "Key Recovery Procedures," item (3), are only a start in this direction. The transfer of keys and functions contemplated in item (3) should "be designed to occur, to the greatest possible extent, without interrupting users' access to information or their ability to export encryption products."

Key Recovery Agent Requirements. While the draft interim regulation acknowledges the possibility of key recovery agents "located outside the U.S." the entire structure is strongly skewed

739

toward U.S. persons and entities. (Relatively few non-U.S. nationals will meet the stated criteria for a key recovery agent, let alone the implicit expectation that such agents will be constantly subject to U.S. civil and criminal jurisdiction.) Prescribing such narrow qualifications for acceptable key recovery agents may pose a problem for the use of key recovery encryption products in foreign jurisdictions that may also wish to ensure their national security and law enforcement agencies' access to encrypted data. Absent bi- or multi-lateral agreements among governments on key recovery or information sharing, narrowly prescribing the nationality of the key recovery agent could effectively result in inconsistent legal commands from authorities with territorial jurisdiction over the foreign branches, offices, subsidiaries and affiliates of U.S. companies using such products. Alternatively, companies may be exposed to key recovery rules and requests from multiple jurisdictions, each requiring secrecy as a condition. Complying with a territorial sovereign's secrecy request during an investigation could, at least theoretically, result in a failure to report or, worse, a false statement to U.S. authorities conducting an audit.

Internal Key Recovery Agents: The Supplement advises that key recovery agents may be "internal to" a user company or organization if such agents can demonstrate sufficient "structural independence" from the rest of the organization. The regulations should expressly state that "internal to" includes company employees. The first sentence of item (a) of the "Key Recovery Agent Requirements" section should be amended to read:

A key recovery agent or key recovery agents may be an employee or employees of or otherwise internal to a user's organization and may consist of one or more individuals.

Corporate employees, officers and directors have fiduciary and other legal duties to such corporations. If BXA's "structural independence" criterion imposes on such officers or employees affirmative obligations to the U.S. government, those obligations should be clearly spelled out to both employee and corporation. An internal recovery agent's duties could theoretically face a conflict of obligations when the government seeks information to be used in investigating the recovery agent's employer. These issues should be addressed:

889

Key Recovery Procedures: Information Sharing: Item (1) of this section prescribes that key recovery agents be able to provide authorized government agencies acting under appropriate legal authority with requested data or material within two hours from the time they receive the request. There is no explanation of why two hours is a relevant or important time period and, on first examination, it seems unreasonably short.

The time period seems even more unreasonable when one takes into account that the information to be provided on such short notice is very broadly defined to include not only requested keys, but "other escrowed material/information available." Requiring key recovery agents to be able to provide on two-hours' notice potentially large volumes of information not precisely defined in advance seems unreasonable.

Recordkeeping: We assume that the data retention requirement in item (2) will be governed by the data retention time periods in the EAR. If any other period (including an indefinite period) is intended, it should be so specified. Any period longer than the EAR-prescribed periods would be objectionable.

It is our impression that requiring long retention periods for some of the categories of information, especially "system administration access" could be unmanageable or, at the least, very complicated and expensive.

Supp. 7 to Part 742: As noted above, the six-month maximum duration for licenses during the two-year transition period is unnaturally short and risks deterring the use of products subject to this regime. It would be preferable if licenses were issued for the entire two-year transition period, but revocable by BXA for cause.

Activities of "U.S. Persons": Since assistance to "foreign persons" could encompass assistance provided within the United States, the definition of "U.S. person" in § 744.9(c)(3) is somewhat awkward. Is a foreign citizen present in the United States a "U.S. person" for purposes of section 744? If so, he or she would arguably not be covered by the general prohibition in § 744.9(a). We assume that BXA intends anyone within the territorial United States to be subject to these restrictions in their capacity as a potential provider/transferor of covered assistance, without

989

changing their status as "foreign persons" in their capacity as recipients. Better drafting should clarify this.

Part 772 Definitions: Given the frequent use of the phrase "object code" in the draft interim regulations, e.g., in the page 6 limitation of the "publicly available" exception, it should be defined.

* * *

EMA looks forward to working further with the Administration to ensure that encryption export policy responds to the concerns of both, the public and private sectors.